Phys 396 2018

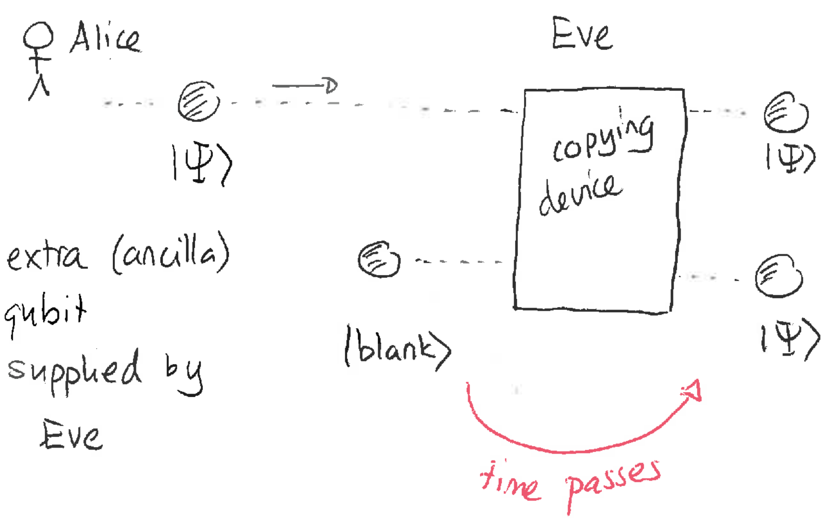
Lecture 14

Tues: HW by 5pm

Also list of possible projects (deadline 9 Nov)

Quantum state evolution

Recall that the cryptography scheme could be subverted if Eve can faithfully copy any of the unknown states that may reach her.



Eve would require a physical device that obeys the laws of quantum physics to actually do this. We must establish whether quantum physics permits this kind of device.

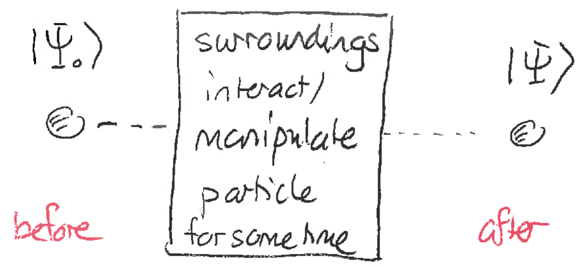
Specifically the device must produce the following state evolution (change as time passes):

$$\underbrace{|\Psi\rangle}_{\text{state sent by Alice}} |blank\rangle \longrightarrow |\Psi\rangle|\Psi\rangle$$

for all possible $|\Psi\rangle$ in $\left\{ |0\rangle, |1\rangle, \frac{|0\rangle+|1\rangle}{\sqrt{2}}, \frac{|0\rangle-|1\rangle}{\sqrt{2}} \right\}$. We would say that such a state clones the qubit Alice sent.

Thus we need to consider a more general question.

Suppose that a quantum system is initially in the state $|\Psi_0\rangle$. The particle is then subjected to external influences or interactions and these produce a "final" state



$|\Psi\rangle$. What are the mathematical rules that decide possibilities for

$$|\Psi_0\rangle \longrightarrow |\Psi\rangle$$

The general rules are as follows:

1) the <u>evolution must be linear</u>

This means that if

$$|\Psi_{01}\rangle \longrightarrow |\Psi_1\rangle$$

and

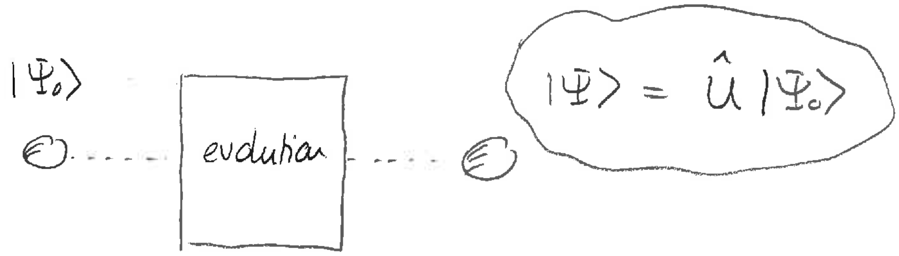
$$|\Psi_{02}\rangle \longrightarrow |\Psi_2\rangle$$

then any combination

$$\alpha_1|\Psi_{01}\rangle + \alpha_2|\Psi_{02}\rangle \longrightarrow \alpha_1|\Psi_1\rangle + \alpha_2|\Psi_2\rangle.$$

This is partly an axiom but one can show that various demands regarding probabilities require such linearity.

Mathematically this means that the evolution can be described by a linear operator (or matrix).



2) the evolution must preserve the normalization.

Thus

$$\langle\Psi|\Psi\rangle = \langle\Psi_0|\Psi_0\rangle$$

Now $\quad \langle\Psi| = (|\Psi\rangle)^{+} = (U|\Psi_0\rangle)^{+} = \langle\Psi_0|\hat{U}^{+}$

where $\hat{U}^{+}$ is the complex conjugate transpose of $\hat{U}$. So for all $|\Psi_0\rangle$ we have

$$\langle\Psi_0|\hat{U}^{+}\hat{U}|\Psi_0\rangle = \langle\Psi_0|\Psi_0\rangle$$

This can only be true for all $|\Psi_0\rangle$ if $\hat{U}^{+}\hat{U} = \hat{I}$, the identity operator.

Thus

$$\boxed{\begin{array}{l}\text{The evolution of a (closed) quantum system is given by} \\ \quad |\Psi_0\rangle \rightarrow |\Psi\rangle = \hat{U}|\Psi_0\rangle \\ \text{where } \hat{U} \text{ is an operator that satisfies:} \\ \quad \hat{U}^{+}\hat{U} = \hat{I}\end{array}}$$

An operator that satisfies $\hat{U}^{+}\hat{U} = \hat{I}$ is called unitary.

1 Evolution

Consider a single qubit subjected to the evolution described by

$$\hat{U} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

in terms of the basis $\{|+\hat{z}\rangle, |-\hat{z}\rangle\}$. For each of the following "initial" states determine the state after evolution.

a) $|\Psi_0\rangle = |0\rangle$.
b) $|\Psi_0\rangle = |1\rangle$.
c) $|\Psi_0\rangle = \dfrac{1}{\sqrt{2}}\left(|0\rangle + |1\rangle\right)$.

Now suppose that a qubit is subjected to the evolution described by

$$\hat{U} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & -1 \\ 1 & 1 \end{pmatrix}$$

in terms of the basis $\{|+\hat{z}\rangle, |-\hat{z}\rangle\}$. For each of the following "initial" states determine the state after evolution.

d) $|\Psi_0\rangle = |0\rangle$.
e) $|\Psi_0\rangle = |1\rangle$.

Answer

a) $|\Psi_0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$ $\quad |\Psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix} = |1\rangle$

b) $|\Psi_0\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$ $\quad |\Psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix} = |0\rangle$

c) $|\Psi_0\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix}$ $\quad |\Psi\rangle = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = |\Psi_0\rangle$

same

d) $\hat{u}^{\dagger}\hat{u} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \hat{I}$

We see that $\hat{u}$ maps

d) $|\Psi_0\rangle = \begin{pmatrix}1\\0\end{pmatrix}$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1&-1\\1&1\end{pmatrix}\begin{pmatrix}1\\0\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(|0\rangle+|1\rangle\right)$$

e) $|\Psi_1\rangle = \begin{pmatrix}0\\1\end{pmatrix}$

$$|\Psi\rangle = \frac{1}{\sqrt{2}}\begin{pmatrix}1&-1\\1&1\end{pmatrix}\begin{pmatrix}0\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\begin{pmatrix}-1\\1\end{pmatrix} = \frac{1}{\sqrt{2}}\left(-|0\rangle+|1\rangle\right)$$

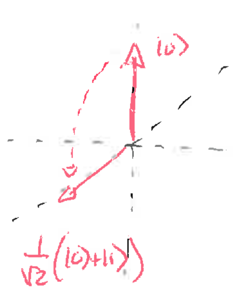
$$= (-1)\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

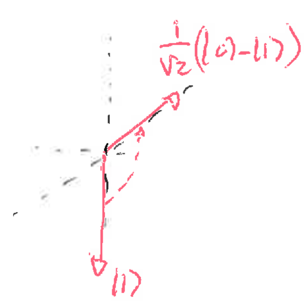
$$= \underbrace{e^{i\pi}}_{\text{global phase}}\frac{1}{\sqrt{2}}\left(|0\rangle-|1\rangle\right)$$

f) $$\hat{U}^\dagger\hat{U} = \frac{1}{\sqrt{2}}\begin{pmatrix}1&1\\-1&1\end{pmatrix}\frac{1}{\sqrt{2}}\begin{pmatrix}1&-1\\1&1\end{pmatrix}$$

$$= \frac{1}{2}\begin{pmatrix}2&0\\0&2\end{pmatrix} = \begin{pmatrix}1&0\\0&1\end{pmatrix}$$

We see that this maps





There are several single qubit unitary operators that arise frequently. Examples are the three Pauli operators:

$$\sigma_x = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad \sigma_y = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix} \qquad \sigma_z = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$$

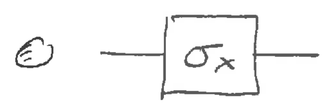
and the Hadamard operator

$$\hat{H} = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$$

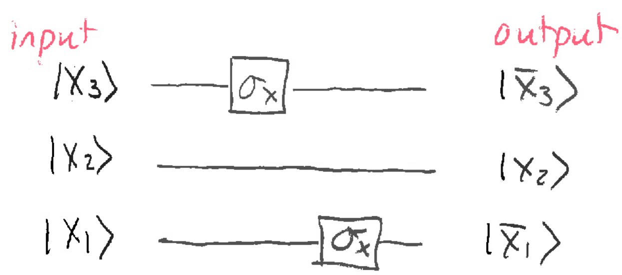
Quantum gates

We can see that for a single qubit the Pauli x operator maps

$$|0\rangle \xrightarrow{\sigma_x} |1\rangle$$
$$|1\rangle \xrightarrow{\sigma_x} |0\rangle \qquad \approx$$



This acts like a NOT gate on a single bit. So if we wanted to do a classical computation that only involved NOT gates we could do this with qubits and Pauli x gates. We can form a circuit:



~~red~~ read left to right

x_1, x_2, x_3 can only be 0, 1

For this reason we call these qubit evolutionary operations quantum gates and we can represent the entire sequence of operations by a quantum circuit.

Single qubit rotation gates.

We can form more general single qubit gates via a process of matrix exponentiation. This uses the Taylor series expansion:

$$e^x = 1 + x + x^2/2! + \frac{x^3}{3!} + \dots = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

and for any matrix $\hat{A}$ we define

$$e^{\hat{A}} := 1 + \hat{A} + \frac{1}{2!}\hat{A}^2 + \dots = \sum \frac{1}{n!}\hat{A}^n$$

We can prove that the exponential obeys the usual rules:

1) $e^{\alpha\hat{A}} e^{\beta\hat{A}} = e^{(\alpha+\beta)\hat{A}}$

2) $(e^{\alpha\hat{A}})^\beta = e^{\alpha\beta\hat{A}}$

3) $\frac{d}{d\alpha}(e^{\alpha\hat{A}}) = \hat{A}e^{\alpha\hat{A}}$

But it does not always satisfy

$$e^{\hat{A}}e^{\hat{B}} \neq e^{\hat{B}}e^{\hat{A}} \neq e^{(\hat{A}+\hat{B})}$$

We will see that generally if $\hat{A}=\hat{A}^\dagger$ then $e^{i\alpha\hat{A}}$ is unitary.

2 Operator exponentiation

a) Show that $\hat{\sigma}_x^2 = \hat{I}$.

b) Determine a matrix expression for

$$\hat{U} = e^{-i\theta\hat{\sigma}_x \cancel{/2}}.$$

Answer: a) $$\sigma_x^2 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \hat{I}$$

b) $$\hat{u} = \hat{I} + (-i\theta\hat{\sigma}_x) + \frac{1}{2!}(-i\theta\hat{\sigma}_x)^2 + \frac{1}{3!}(-i\theta\hat{\sigma}_x)^3 + \dots$$

$$= \hat{I} - i\theta\hat{\sigma}_x + \frac{1}{2!}(-\theta^2)\hat{I} + \frac{1}{3!}(-i)^3\theta^3 \underbrace{\hat{\sigma}_x^2}_{\hat{I}}\hat{\sigma}_x + \dots$$

$$= \hat{I}\left(1 - \frac{1}{2!}\theta^2 + \frac{1}{4!}\theta^4\right) + \dots$$

$$-i\hat{\sigma}_x\left(\theta - \frac{1}{3!}\theta^3 + \dots\right)$$

$$= \hat{I}\cos\theta - i\sigma_x\sin\theta$$

$$\hat{u} = \begin{pmatrix} \cos\theta & -i\sin\theta \\ -i\sin\theta & \cos\theta \end{pmatrix}$$

Now consider an operator

$$\hat{U} = e^{-i\varphi\hat{\sigma}_x/2} = \begin{pmatrix} \cos\varphi/2 & -i\sin\varphi/2 \\ -i\sin\varphi/2 & \cos\varphi/2 \end{pmatrix}$$

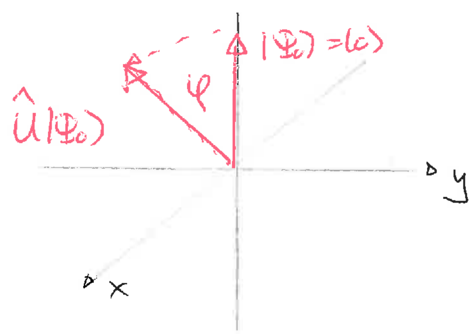
Then acting on the initial state $|0\rangle$ this produces

$$\hat{U}|0\rangle = \begin{pmatrix} \cos\varphi/2 \\ -i\sin\varphi/2 \end{pmatrix} = \cos\varphi/2\,|0\rangle - i\sin\varphi/2\,|1\rangle$$

$$= \cos\varphi/2\,|0\rangle + e^{i3\pi/2}\sin\varphi/2\,|1\rangle.$$

This is the Bloch sphere state with parameters $\theta = \varphi$, $\phi = 3\pi/2$

So this operation performs a rotation about the x axis through angle φ



Some moderately involved mathematics results in the fact that

Every single qubit unitary operation can be represented as a rotation in the Bloch sphere.